Amendments to the Specification

Please amend the specification as follows.

Please make the indicated changes to the Abstract:

The invention relates to a method ~~whereby it can be checked whether~~ to verify that data received by a receiver has been sent by a transmitter authorized by a trusted third party, the transmitter and the receiver being connected to a digital network. An identifier is associated with the data sent by the transmitter and, on receipt of the data by the receiver, the receiver generates a random number and diffuses the same on the network. The transmitter that receives ~~said~~ the random number calculates a response by applying a first function to the random number and to the identifier, and sends ~~said~~ the response to the receiver which verifies the response received by applying a second function to the response received, the random number and the identifier. The first function is delivered first to the transmitter by the trusted third ~~part~~ party. [[,]] ~~and the~~ The second function is a function for checking the result of the first function which is delivered first to the receiver by the ~~thrusted~~ trusted third party.

Please make the indicated changes to paragraph on page 6, beginning on line 10 of the Specification as follows:

A function G corresponding to the above definition may in particular be an encryption function such as the AES function described in particular in "FIPS 197: Specification of the Advanced Encryption Standard (AES) - 26 November 2001"~~ available at the following Internet address: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf~~. It may also be a hashing function such as the HMAC-SHA1 function described in particular in "FIPS Publication 198: The Keyed-Hash Message Authentication Code (HMAC), National Institute of Standards and Technology, 2001"~~ available at the following Internet address: http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf~~.